

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

7



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/588,049      | 06/06/2000  | MASAKI KYOJIMA       | 106406              | 8128             |

25944 7590 08/09/2004  
OLIFF & BERRIDGE, PLC  
P.O. BOX 19928  
ALEXANDRIA, VA 22320

EXAMINER

LANIER, BENJAMIN E

ART UNIT PAPER NUMBER

2132

DATE MAILED: 08/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

7

# Office Action Summary

Application No.

09/588,049

Applicant(s)

KYOJIMA ET AL.

Examiner

Benjamin E Lanier

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 17 June 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1,3-10 and 12-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,3-10 and 12-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 June 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. §§ 119 and 120

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☒ All b) ☐ Some \* c) ☐ None of:  
1. ☒ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.  
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

## Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_ 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Amendment***

1. Applicant's amendment of claims 1, 5, 9, 10, 14, 18, 19, 23, 30 has been fully considered and is entered.

### ***Response to Arguments***

2. Applicant's arguments filed 17 June 2004 have been fully considered but they are not persuasive. Applicant's argument that the Boebert and Deo references do not disclose key generation using a one-way function is not persuasive because Deo discloses that the encryption keys are generated using a Message Authentication Code (Col. 24, lines 32-54). Message Authentication Codes are one-way hash functions.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claims 1, 3, 4-10, 12-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boebert, U.S. Patent No. 5,502,766, in view of Deo, U.S. Patent No.

Art Unit: 2132

6,496,928. Referring to claims 1, 2, 5, 6, 8-10, 12, 14, 15, 17-27, 29-32, Boebert discloses a data enclave system wherein a workstation user's ID and PIN, stored in the memory of their Personal Keying Device (data-for-second-checking memory unit), is used to generate an encryption key (Col. 10, lines 22-34), which meets the limitation key generation unit for generating an encrypting key from data stored in the data-for-secondary-checking memory unit. The generated encryption key is the used to encrypted the access vector and media key that is stored in the storage search logic (data-for-main-checking memory unit)(Col. 13, lines 42-57), which meets the limitation of an encryptor for encrypting data stored in the data-for-main-checking memory unit with the encrypting key generated by the encrypting key generation unit. Authentication protocols are executed with the use of two pseudo random number sequences (Col. 26, lines 44-47). The enciphered Media key and access vector pair arrives at the Crypto Media Controller and the Media ID is used as an index to store the enciphered pair packet in the Personal Keying Device of the user. The media can now be identified and the individual Personal Keying Device contains a media key which can only be used by someone who has physical possession of that Personal Keying Device, knows that individuals PIN, and has the Media of controlled by a Crypto Media Controller containing the enclave key (Col. 13, line 64 – Col. 14, line 13), which meets the limitations of the data verification between units. Boebert discloses that keys can be stored in a database (key memory) for later use (Col. 26, lines 8-13). Boebert does not disclose that the stored keys can be used to generate new keys. Deo discloses the use of old keys that are hashed with other data (data for secondary checking memory unit) to generate new encryption keys (Col. 24, lines 32-54), which meets the limitation of the encryption key generation unit also uses

Art Unit: 2132

the previous key stored in the previous key memory unit in generating the encrypting key. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the old keys of Boebert to generate new keys in the manner of Deo in order to increase the difficulty of the key becoming compromised as disclosed in Deo (Col. 24, lines 57-68).

Referring to claim 4, 13, Boebert discloses that digital signatures can be used in the data enclave system (Col. 23, lines 50-53).

Referring to claims 7, 16, 28, Boebert discloses using symmetric encryption (Col. 9, lines 22 – Col. 10, line 10).

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

### *Conclusion*

Art Unit: 2132

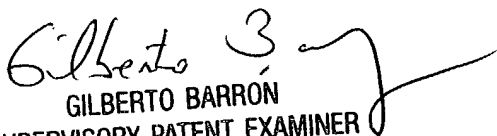
7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 703-305-7684. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703)305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier



GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100